



Fundusze Europejskie  
dla Podkarpacia



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



PODKARPACKIE  
przestrzeń otwarta

Numer sprawy: OA.132.9.2024

Łańcut, dnia 30 września 2024 r.

## Szczegółowy Opis Przedmiotu Zamówienia

pn. Dostawa i wdrożenie licencji  
oprogramowania wraz z przeprowadzeniem  
niezbędnych szkoleń

## Spis treści

1. Zestawienie ilościowe.....	3
2. Zasada równoważności rozwiązań i neutralności technologicznej. ....	4
3. Wymagania ogólne w zakresie dostawy oprogramowania.....	6
4. Przedmiot zamówienia dla części nr 1.....	10
4.1. Dostawa licencji na system operacyjny do serwerów (2 szt.). ....	10
4.2. Dostawa licencji na system do wirtualizacji (1 szt.). ....	18
4.3. Dostawa licencji na system backup (1 szt.). ....	21
4.4. Dostawa licencji na program antywirusowy (150 szt.).....	26
5. Przedmiot zamówienia dla części nr 2.....	35
5.1. Dostawa licencji zapory sieciowej UTM (2 szt.).....	35
5.2. Dostawa licencji oprogramowania do zbierania i przechowywania logów z urządzeń UTM (1 szt.). 40	
6. Przedmiot zamówienia dla części nr 3.....	41
6.1. Dostawa licencji oprogramowania do monitorowania i analizy cyberbezpieczeństwa (1 szt.). ...	41
6.2. Zakup usług szkoleń z zakresu oprogramowania do monitorowania i analizy cyberbezpieczeństwa (30 godz.). ....	57

## 1. Zestawienie ilościowe.

Część nr 1 – Dostawa licencji na system operacyjny do serwerów, licencji na system do wirtualizacji, licencji na system do backup, licencji na system antywirusowy.

Lp.	Nazwa	Ilość
1.	Dostawa licencji na system operacyjny do serwerów	2 szt.
2.	Dostawa licencji na system do wirtualizacji	1 szt.
3.	Dostawa licencji na system backup	1 szt.
4.	Dostawa licencji na program antywirusowy	150 szt.

Część nr 2 – Dostawa licencji dla zapory sieciowej UTM oraz licencji na oprogramowanie do zbierania i przechowywania logów z urządzeń UTM.

Lp.	Nazwa	Ilość
1.	Dostawa licencji zapory sieciowej UTM	2 szt.
2.	Dostawa licencji oprogramowania do zbierania i przechowywania logów z urządzeń UTM	1 szt.

Część nr 3 – Dostawa licencji oprogramowania do monitorowania i analizy cyberbezpieczeństwa, szkolenia administratorów i użytkowników.

Lp.	Nazwa	Ilość
1.	Dostawa licencji oprogramowania do monitorowania i analizy cyberbezpieczeństwa	1 szt.
2.	Zakup usług szkoleń z zakresu oprogramowania do monitorowania i analizy cyberbezpieczeństwa	30 godz.

## 2. Zasada równoważności rozwiązań i neutralności technologicznej.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań lub też stosowane jest w celu wskazania aktualnie użytkowanego środowiska Zamawiającego, z którym rozwiązanie równoważne powinno być kompatybilne.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.
5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.
9. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których

mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

### 3. Wymagania ogólne w zakresie dostawy oprogramowania.

1. Dostarczone oprogramowanie musi być wolne od wad prawnych i fizycznych oraz wcześniej nieużytkowane.
2. Dostarczone oprogramowanie musi być fabrycznie nowe, musi pochodzić z oficjalnego kanału sprzedaży producenta, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta oferowanego oprogramowania.
3. Niedopuszczalne są produkty prototypowe oraz pochodzących z programów wyprzedażowych producenta. Oferowane oprogramowanie nie może znajdować się na liście „end-of-sale”, „end-of-life” oraz „end-of-support” producenta.
4. Wykonawca zapewni dostawę oprogramowania do wskazanej lokalizacji w siedzibie Zamawiającego.
5. Wykonawca jest odpowiedzialny za skonfigurowanie w porozumieniu z Zamawiającym oprogramowania w celu przygotowania zamawianego oprogramowania do działania.
6. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
7. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji oprogramowania.
8. Dla dostaw oprogramowania Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania, nieużywanego oraz nigdy wcześniej nieaktywowanego oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania posiadającego fizyczny nośnik naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
9. Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:
  - a. Instalacja ma odbyć się na komputerach oraz serwerach wskazanych przez Zamawiającego, a w przypadku, jeżeli dostarczone oprogramowanie działa w modelu rozwiązania chmurowego to Wykonawca jest zobligowany do konfiguracji oprogramowania w chmurze Wykonawcy bądź Producenta oferowanego oprogramowania.
  - b. Zamawiający dopuszcza instalację i wdrożenie zdalne przy wykorzystaniu narzędzia Wykonawcy, z zastrzeżeniem, że Wykonawca jest zobowiązany dostarczyć oprogramowanie do zdalnej pracy umożliwiające szyfrowanie połączeń oraz nagrywanie sesji serwisowych.
  - c. W przypadku, jeżeli dotyczy, Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.
  - d. Usługa wdrożenia obejmuje:
    - i. przeprowadzenie analizy przedwdrożeniowej,

- ii. instalację silnika bazy danych – jeżeli będzie wymagana instalacja,
  - iii. rejestracja produktu – jeżeli wymagana,
  - iv. instalację oprogramowania: na stacji roboczej lub serwerze – jeżeli dotyczy,
  - v. dystrybucję oprogramowania na wybranych stacjach roboczych – jeżeli dotyczy,
  - vi. konfigurację oprogramowania,
  - vii. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego,
  - viii. szkolenie administratorów z zakresu pracy z programem,
  - ix. w uzgodnionym terminie z Zamawiającym zostanie przeprowadzane kontrolne połączenie zdalne w celu weryfikacji ustawień oraz poprawienia konfiguracji.
10. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia oprogramowania – wymagania minimalne:
- a. Wykonawca przygotowuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego oprogramowania, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uwzględniające obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
    - i. scenariusze testowe, procedury oraz wzory raportów testów,
    - ii. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
    - iii. opis koncepcji realizacji prac,
    - iv. zalecenia przedwdrożeńowe dla Zamawiającego, jeżeli będą wymagane.
  - b. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
    - i. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 10 dni kalendarzowych od dnia zawarcia umowy,
    - ii. Zamawiający w terminie nie dłuższym niż 5 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
    - iii. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 4 dni roboczych od dnia ich otrzymania,
    - iv. Zamawiający w terminie 4 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
    - v. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
    - vi. zatwierdzony projekt techniczny wraz z procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej, w postaci plików do edycji i PDF.
  - c. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.
  - d. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.

- e. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
  - f. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery”. Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.
11. Instruktaże w zakresie dostarczonego oprogramowania – wymagania ogólne minimalne:
- a. Instruktaże stanowiskowe będą prowadzone w języku polskim w siedzibie Zamawiającego i obejmą zakresem m.in.: użytkowane oprogramowanie; budowę, architekturę i konfigurację rozwiązania; administrowanie wdrożonym rozwiązaniem.
  - b. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
  - c. O ile w dokumencie nie wskazano inaczej, instruktaże powinny trwać minimum 8 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób.
  - d. Zamawiający dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
  - e. Administratorzy rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne, a także instalacji oprogramowania, znać i umieć realizować procedury backupu. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem rozwiązania, a także sposoby ich przeciwdziałania, wykrywania i usuwania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować wdrożone rozwiązanie, jak również znać jego wdrożoną konfigurację.
12. Wymagania licencyjne dla dostarczonego oprogramowania:
- a. Licencjobiorcą wszystkich licencji będzie Miasto Łańcut. W przypadku licencji systemu antywirusowego licencje mogą zostać wykorzystane na rzecz jednostek podległych Miasta Łańcut.
  - b. Zamawiający dopuszcza udzielenie licencji w wersji papierowej i/lub elektronicznej. W przypadku, jeżeli producent oprogramowania nie wystawia licencji w zakresie oferowanego oprogramowania Wykonawca powinien dostarczyć stosowne oświadczenie producenta oprogramowania bądź jego dystrybutora.
  - c. Licencje muszą obowiązywać w okresie 24 miesięcy od dnia odbioru przedmiotu zamówienia przez Zamawiającego niezależnie od modeli dystrybucji poszczególnych producentów oferowanego oprogramowania.
  - d. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
  - e. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do przeniesienia oprogramowania na inny serwer/komputer.
  - f. Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet). Użytkownik może pracować w dowolny dostępny technologicznie sposób.



- g. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
  - h. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
  - i. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym urządzeniu klienckim (licencja nie może być przypisana do komputera/urządzenia).
  - j. Wykonawca zapewni aktualizację oprogramowania do najnowszej wersji oprogramowania w okresie ważności licencji.
13. Wymagania gwarancyjne dla dostarczonego oprogramowania:
- a. Zamawiający wymaga dostarczenia gwarancji producenta oferowanego oprogramowania. Zamawiający nie dopuszcza gwarancji Wykonawcy.
  - b. Gwarancja producenta musi zostać zapewniona przez Wykonawcę na oferowane oprogramowanie na okres 24 miesięcy od dnia odbioru przedmiotu zamówienia przez Zamawiającego.
  - c. Gwarancja producenta musi umożliwiać Zamawiającemu zgłaszanie błędów w oprogramowaniu.
14. Wymagania wsparcia technicznego dla dostarczonego oprogramowania:
- a. Zamawiający wymaga usług świadczenia wsparcia technicznego oferowanego oprogramowania. Zamawiający dopuszcza świadczenie usług wsparcia technicznego przez Wykonawcę, Producenta lub Autoryzowanego Przedstawiciela Producenta.
  - b. Świadczenie usług wsparcia technicznego musi zostać zapewnione przez Wykonawcę na oferowane oprogramowanie na okres 24 miesięcy od dnia odbioru przedmiotu zamówienia przez Zamawiającego.
  - c. Świadczenie usług wsparcia technicznego polegać będzie na wsparciu telefonicznym w zakresie oferowanego oprogramowania dotyczącym prawidłowego i zgodnego z wymaganiami producenta użytkowania oprogramowania.
  - d. Dla części nr 1 Zamawiający wymaga w ramach wsparcia technicznego zapewnienia przez Wykonawcę do dnia 31.12.2025 r. dodatkowych usług konfiguracyjnych dostarczonego oprogramowania polegających minimum na tworzeniu maszyn wirtualnych na potrzeby planowanego do wdrożenia systemu informacji przestrzennej (SIP); tworzeniu i przydzielaniu zasobów dyskowych dla SIP; konfiguracji backup oprogramowania i zasobów danych SIP oraz innych wymagań konfiguracyjnych dotyczących dostarczanego oprogramowania i określonych przez Zamawiającego w celu wdrożenia oprogramowania SIP.
15. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi”, „powinien”, „możliwość” określając w ten sposób wymaganą funkcjonalność oprogramowania.

## 4. Przedmiot zamówienia dla części nr 1.

### 4.1. Dostawa licencji na system operacyjny do serwerów (2 szt.).

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie 1000 instancji wirtualnych tego serwerowego systemu operacyjnego na dwóch serwerach dwuprocessorowych o 8 rdzeniach każdy procesor pracujących w klastrze. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na istniejących serwerach.

Minimalne wymagania funkcjonalne systemu operacyjnego do serwerów:

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
  - a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
  - b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
  - c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
  - d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
  - a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
  - b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
  - a) Login i hasło,
  - b) Karty z certyfikatami (smartcard),
  - c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
  - a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
  - b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
    - i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
    - ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
    - iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
    - iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1,
    - v. możliwość uruchomienia usługi katalogowej w trybie usługi,
    - vi. możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń,
    - vii. możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem (w tym przynależność do grup zabezpieczeń),
    - viii. możliwość zarządzania usługą katalogową poprzez interfejs graficzny oraz CLI,

- ix. możliwość zainstalowania lokalnego Centrum Certyfikacji zapewniającego wydawanie niekwalifikowanych certyfikatów X.509 umożliwiających uwierzytelnianie na stacjach roboczych i serwerach z wykorzystaniem kart kryptograficznych, szyfrowanie danych.
- c) Zdalna dystrybucja oprogramowania na stacje robocze,
- d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
- e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
  - i. Dystrybucję certyfikatów poprzez http,
  - ii. Konsolidację CA dla wielu lasów domeny,
  - iii. Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen,
  - iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
- f) Szyfrowanie plików i folderów,
- g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
- h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
- i) Serwis udostępniania stron WWW,
- j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
- k) Wsparcie dla algorytmów Suite B (RFC 4869),
- l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
  - i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
  - ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych,
  - iii. Obsługi 4-KB sektorów dysków,
  - iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
  - v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,
  - vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode).
- 26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
- 27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
- 28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31. Dostępność zorganizowanego systemu szkoleń producenta oprogramowania i materiały edukacyjne w języku polskim.
32. Wykonawca jest zobowiązany dostarczyć licencje dostępne do oferowanych systemów operacyjnych w ilości 90 szt. Oferowane licencje muszą udostępnić możliwość korzystania z zasobów serwisów 90 użytkownikom.

W ramach dostawy systemu operacyjnego Wykonawca jest zobowiązany do przeprowadzenia usług rekonfiguracyjnych i wdrożeniowych, aktualizacji usługi katalogowej wraz z dodatkowymi komponentami w zakresie:

1. Zaplanowania liczby serwerów na potrzeby usługi katalogowej oraz serwerów plików. Zamawiający wymaga, aby zaplanowano taką liczbę serwerów, aby w przypadku awarii pojedynczego serwera był zapewniony ciągły dostęp do usługi katalogowej, a w szczególności mechanizmy uwierzytelniania oraz rozwiązywania nazw oraz serwera plików. Zamawiający dopuszcza wykorzystanie serwerów wirtualnych uruchomionych na dostarczonym środowisku wirtualizacyjnym.
2. Instalacja systemu operacyjnego serwerów. Instalacja systemu operacyjnego serwerów w taki sposób, aby w łatwy sposób możliwe było włączenie funkcji szyfrowania partycji systemowej za pomocą wbudowanych w system operacyjny mechanizmów. Po instalacji systemy operacyjne muszą zostać prawidłowo aktywowane. Następnie należy zainstalować niezbędne aktualizacje oraz poprawki związane z bezpieczeństwem udostępnione przez producenta systemu operacyjnego.
3. Uruchomienie usługi katalogowej oraz niezbędnych komponentów, migracja danych do/z obecnej usługi katalogowej. Usługa katalogowa musi być uruchomiona na wszystkich serwerach przewidzianych do rozbudowy. Na wszystkich serwerach muszą być uruchomione także komponenty odpowiedzialne za rozwiązywanie nazw. Należy szczególną uwagę zwrócić na poprawne funkcjonowanie mechanizmów replikacji. Usługę katalogową należy skonfigurować w taki sposób, aby możliwe było wykorzystanie możliwie wszystkich funkcjonalności oferowanych przez zastosowane systemy operacyjne, a w szczególności możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń, możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem. W ramach prac Wykonawca utworzy strukturę jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego.
4. Zamawiający wymaga skonfigurowania delegacji uprawnień do zadanych jednostek organizacyjnych dla administratorów niższego poziomu. Administratorzy niższego poziomu powinni mieć uprawnienia do:
  - a) Resetowania haseł użytkowników
  - b) Odblokowywania kont użytkowników
  - c) Zmiany atrybutów „Display Name” oraz „Last name”
5. Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi:

- a) Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości
  - b) Śledzenie zmian dotyczących tworzenia, usuwania obiektów
6. Zamawiający wymaga skonfigurowania dwóch stacji zarządzających. Zarządzanie środowiskiem będzie się odbywać z poziomu stacji zarządzających (usługa katalogowa, wszystkie możliwe do zarządzania z poziomu stacji zarządzającej komponenty serwerów).
7. Zamawiający wymaga skonfigurowania globalnej polityki haseł dla domeny:
- a) Hasło musi zawierać minimum 10 znaków,
  - b) Maksymalny czas ważności hasła: do ustalenia z Zamawiającym,
  - c) Minimalny czas, po którym możliwa jest zmiana hasła: do ustalenia z Zamawiającym,
  - d) Hasło musi spełniać zasady złożoności,
  - e) Po 3 nieudanych próbach uwierzytelniania konto powinno być blokowane na 30 minut. Automatyczne anulowanie blokady ma następować po 480 minutach.
8. Zamawiający wymaga skonfigurowania polityki haseł dla kadry zarządzającej:
- a) Hasło musi zawierać minimum 14 znaków,
  - b) Maksymalny czas ważności hasła: 30 dni,
  - c) Minimalny czas, po którym możliwa jest zmiana hasła: 240 dni,
  - d) Hasło musi spełniać zasady złożoności.
9. Zamawiający wymaga skonfigurowania polityki haseł tak, by po 3 nieudanych próbach uwierzytelniania konto powinno być blokowane na 30 minut. Automatyczne anulowanie blokady ma następować po 480 minutach.
10. Zamawiający wymaga stworzenia nowych kont użytkowników, grup zabezpieczeń oraz jednostek organizacyjnych. Zamawiający oczekuje stworzenia przez Wykonawcę skryptów ułatwiających te zadania zgodnie z wymaganiami poniżej:
- 10.1. Założenia skryptu tworzącego nowe jednostki organizacyjne oraz grupy:
- 10.1.1. Możliwość skonfigurowania za pomocą zmiennych w skrypcie, co najmniej:
    - a) ścieżki i nazwy pliku wejściowego,
    - b) ścieżki i nazwy pliku logującego,
    - c) ścieżki i nazwy pliku wyjściowego (właściwego skryptu),
    - d) nazwy FQDN domeny,
    - e) nazwy NetBIOS domeny,
    - f) nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty,
    - g) ścieżek do udziałów dyskowych SHARE1 oraz SHARE2,
  - 10.1.2. Skrypt ma pobierać z pliku wejściowego listę jednostek organizacyjnych.
  - 10.1.3. Skrypt tworzy nowe jednostki organizacyjne w jednostce organizacyjnej nadrzędnej zdefiniowanej w części konfiguracyjnej skryptu.
  - 10.1.4. Skrypt tworzy nowe grupy zabezpieczeń o nazwie G\_Nazwa\_Jednoski\_Organizacyjnej.
  - 10.1.5. Skrypt tworzy foldery:
    - a) \\DOMENA\Public\SHARE1,
    - b) \\DOMENA\Public\SHARE2.Foldery muszą posiadać tak ustawione parametry zabezpieczeń, aby użytkownicy nie mogli samodzielnie tworzyć nowych katalogów ani plików w lokalizacjach \\DOMENA\SHARE1 oraz \\DOMENA\SHARE2.

10.1.6. Skrypt tworzy podkatalogi:

\\DOMENA\Public\SHARE1\Nazwa\_Jednostki\_Organizacyjnej oraz  
\\DOMENA\Public\SHARE2\Nazwa\_Jednostki\_Organizacyjnej.

10.1.7. Skrypt nadaje uprawnienia do utworzonych podkatalogów według założeń:

a) \\DOMENA\Public\SHARE1\Nazwa\_Jednostki\_Organizacyjnej:

- i. Administratorzy Domeny – Pełna kontrola,
- ii. Grupa G\_Nazwa\_Jednostki\_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa\_Jednostki\_Organizacyjnej,
- iii. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu,
- iv. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze.

b) \\DOMENA\Public\Share2\Nazwa\_Jednostki\_Organizacyjnej:

- i. Administratorzy Domeny – Pełna kontrola,
- ii. Grupa G\_Nazwa\_Jednostki\_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa\_Jednostki\_Organizacyjnej
- iii. Użytkownicy Uwierzytelnieni – Odczyt,
- iv. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu,
- v. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze.

10.1.8. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina).

10.1.9. Działanie skryptu właściwego musi być w całości logowane do pliku tekstowego, opatrzonego bieżącą datą i godziną w celu umożliwienia każdorazowego zweryfikowania poprawności działania.

10.2. Założenia skryptu tworzącego nowe konta użytkowników:

10.2.1. Możliwość skonfigurowania za pomocą zmiennych w skrypcie co najmniej:

- a) ścieżki i nazwy pliku wejściowego,
- b) ścieżki i nazwy pliku logującego,
- c) ścieżki i nazwy pliku wyjściowego (właściwego skryptu),
- d) nazwy FQDN domeny,
- e) nazwy NetBIOS domeny,
- f) nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty,
- g) ścieżki do udziału sieciowego HOME,
- h) litery dysku katalogu domowego.

10.2.2. Skrypt ma pobierać z pliku wejściowego listę kont użytkowników w formacie:

NazwaUzytkownika; Imie; Nazwisko: Haslo; Dzial; NumerTelefonu

10.2.3. Skrypt tworzy nowe konta użytkowników w jednostce organizacyjnej nadrzędnej zdefiniowanej w części konfiguracyjnej skryptu pobierając wszystkie niezbędne dane z pliku wejściowego

- 10.2.4. Nowo utworzone konta użytkowników muszą mieć jednorazowo ustawione hasła – użytkownik musi zmienić hasło podczas pierwszego logowania
- 10.2.5. Skrypt tworzy katalog \\DOMENA\HOME\NazwaUzytkownika
- 10.2.6. Skrypt nadaje uprawnienia do utworzonych katalogów użytkowników według założeń:
- a) Administratorzy Domeny – Pełna kontrola,
  - b) Użytkownik – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu NazwaUzytkownika,
  - c) Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu,
  - d) Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze.
- 10.2.7. Skrypt ma ustawić dla każdego konta użytkownika literę dysku domowego oraz poprawną ścieżkę sieciową
- 10.2.8. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina)
- 10.2.9. Działanie skryptu właściwego musi być w całości logowane do pliku tekstowego, opatrzonego bieżącą datą i godziną w celu umożliwienia każdorazowego zweryfikowania poprawności działania
- 10.2.10. Skrypt ma wygenerować dla każdego zakładanego konta osobny plik tekstowy zawierający między innymi: Nazwę użytkownika, Imię, Nazwisko, Hasło do pierwszego zalogowania. Tak utworzone pliki mogą zostać wydrukowane i przekazane użytkownikom.
- 10.3. Powyżej opisane skrypty muszą posiadać w treści kodu stosowne komentarze opisujące działanie skryptów. Skrypty zostaną przekazane Zamawiającemu w wieczyste użytkowanie bez dodatkowych opłat wraz ze stosowną dokumentacją użytkownika oraz szczegółową instrukcją obsługi.
- 10.4. Zamawiający wymaga wygenerowania kont użytkowników, katalogów domowych użytkowników, jednostek organizacyjnych, grup zabezpieczeń za pomocą opracowanych skryptów.
11. Zamawiający wymaga skonfigurowania mechanizmów mapowania dysków sieciowych dla systemów klienckich Windows.
12. Mapowane mają być między innymi zasoby: \\DOMENA\Public\SHARE1; \\DOMENA\Public\SHARE2 oraz określone przez Zamawiającego drukarki sieciowe.
13. Zamawiający wymaga skonfigurowanie mapowania dysków sieciowych za pomocą zasad grup na dwa sposoby:
- a) z wykorzystaniem skryptów logowania,
  - b) z wykorzystaniem mechanizmów zaimplementowanych w systemach Microsoft Windows Vista i nowszych (Wymagane jest także skonfigurowanie automatycznej instalacji niezbędnych składników na stacjach klienckich. Zamawiający nie dopuszcza instalacji wymaganych składników ręcznie).
14. Zamawiający wymaga uruchomienia oraz skonfigurowania serwerów plików oraz serwerów wydruków.
15. Serwery plików muszą być skonfigurowane z wykorzystaniem dostępnych w zaoferowanych systemach operacyjnych serwerów mechanizmów zwiększających dostępność danych poprzez zastosowanie technologii replikacji systemu plików. Konieczność taka podyktowana jest



zapewnieniem ciągłości dostępu do krytycznych danych Zamawiającego w przypadku awarii jednego z serwera plików. Zastosowane mechanizmy replikacji systemu plików muszą zapewniać:

- a) Replikację multi-master z rozwiązywaniem konfliktów
- b) Wykorzystanie algorytmów kompresji danych wykrywających zmiany na poziomie bloków danych w obrębie plików – replikacji podlegają tylko zmienione bloki danych, a nie całe pliki.

16. Serwery plików muszą być skonfigurowane w taki sposób, aby ograniczać ekspozycję danych dla użytkowników oraz grup, które nie mają do nich dostępu.
17. Na serwerach plików muszą być skonfigurowane przydziały dyskowe dla użytkowników i grup. Zamawiający wymaga także skonfigurowania przydziałów dyskowych dla wskazanych folderów.
18. Zamawiający wymaga włączenia i skonfigurowania mechanizmów uniemożliwiających przechowywanie niedozwolonych typów plików. Konieczne jest także skonfigurowanie mechanizmów raportujących.
19. Zamawiający wymaga skonfigurowania mechanizmów przekierowania lokalnych folderów „Moje Dokumenty” oraz „Pulpit” ze stacji roboczych na serwery plików. Funkcjonalność ta musi poprawnie działać dla systemów klienckich Zamawiającego.
20. Zamawiający wymaga stworzenia domyślnego, obowiązującego profilu wędrującego dla klienckich systemów operacyjnych. Domyślny profil ma uwzględniać opracowanie i wykonanie grafiki na pulpit komputera klienta. Grafika będzie akceptowana przez Zamawiającego. Zamawiający wymaga stworzenia i przypisania odpowiednich polityk globalnych dla wymuszenia stosowania obowiązkowych (niemodyfikowalnych) profili mobilnych.
21. Zamawiający wymaga opracowania koszyka dozwolonych aplikacji wraz z implementacją polityk globalnych ograniczających dostęp do aplikacji z wykorzystaniem np.: dedykowanych ustawień związanych z polityką kontroli uruchomienia aplikacji.
22. Zamawiający wymaga skonfigurowania parametrów audytu dla serwerów plików umożliwiających minimum:
  - a) Określenie daty, czasu, nazwy użytkownika, który usunął / próbował usunąć plik/folder,
  - b) Określenie daty, czasu, nazwy użytkownika, który zapisał / próbował zapisać plik/folder,
  - c) Określenia daty, czasu, nazwy użytkownika, który próbował uzyskać nieuprawniony dostęp do zasobów, do których nie ma uprawnień.
23. Zamawiający wymaga uruchomienia serwera wydruków oraz podłączenia i skonfigurowania drukarek sieciowych. Zamawiający wymaga opracowania i skonfigurowania odpowiednich polityk globalnych mapujących odpowiednie drukarki użytkownikom. Niedopuszczalne jest przyłączenie wszystkim użytkownikom wszystkich dostępnych drukarek. Użytkownicy powinni mieć przyłączone drukarki znajdujące się najbliżej jego komputera.
24. Zamawiający wymaga uruchomienia serwerów uwierzytelniających współpracujących z infrastrukturą AD, realizujących funkcję uwierzytelniania na dostarczanych przełącznikach sieciowych.
25. Zamawiający wymaga uruchomienia co najmniej dwóch instancji serwera uwierzytelniania w celu zachowania redundancji na dwóch niezależnych serwerach.
26. Instancja serwera może być uruchomiona na serwerach domenowych z zastrzeżeniem, że będzie ona kompatybilna z usługami uruchomionymi na tych serwerach i nie będzie wpływać negatywnie na ich pracę.

27. Zamawiający wymaga skonfigurowania odpowiednich polityk bezpieczeństwa na zainstalowanych serwerach uwierzytelniających bazujących na utworzonych w strukturze usługi katalogowej Zamawiającego grupach.
28. Jeżeli jest potrzebna, Zamawiający wymaga dostarczenia licencji na instalowane serwery uwierzytelniające oraz ujęcia ich ceny w ofercie.
29. Zamawiający wymaga uruchomienia i skonfigurowania usług dostępnych w dostarczonych systemach operacyjnych serwerów umożliwiających zarządzanie aktualizacjami stacji roboczych i serwerów Windows w zakresie minimum:
  - a) Aktualizacje i poprawki mają być pobierane na serwer instalacyjny za pośrednictwem sieci Internet,
  - b) Administrator zatwierdza aktualizacje do instalacji,
  - c) Stacje robocze i serwery pobierają i automatycznie instalują zatwierdzone przez Administratora aktualizacje według określonego harmonogramu.
30. Zamawiający wymaga skonfigurowania co najmniej następujących parametrów:
  - a) Systemów operacyjnych, aplikacji oraz wersji językowych, dla których będą pobierane aktualizacje,
  - b) Kategorii aktualizacji,
  - c) Grup komputerów (KOMPUTERY, SERWERY, KOMPUTERY-TEST, SERWERY-TEST),
  - d) Polityk globalnych przypisujących komputery znajdujące się w określonych jednostkach organizacyjnych do odpowiednich grup komputerów,
  - e) Zasad automatycznego zatwierdzania nowych aktualizacji,
  - f) Mechanizmów raportowania (email).

## 4.2. Dostawa licencji na system do wirtualizacji (1 szt.).

Zamawiający posiada licencję oprogramowania VMware - Essentials Plus. Przedmiotem zamówienia jest przedłużenie istniejącej u Zamawiającego licencji oprogramowania do wirtualizacji VMware w wersji Essentials Plus pozwalające na użytkowanie najnowszej wersji programu w okresie 24 miesięcy dla 3 serwerów fizycznych posiadających 2 procesory lub dostawy równoważnego systemu wirtualizacji zgodnie z poniżej wskazanymi kryteriami równoważności.

Kryteria równoważności dla dostawy licencji przedłużającej oprogramowanie do wirtualizacji VMware w wersji Essentials Plus realizowanej przez dostawę równoważnego systemu wirtualizacji:

1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3. Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
4. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych.

6. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM.
8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowo.
10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
11. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
12. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SLES, RHEL, Solaris, OS/2, NetWare, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu SCO OpenServer, SCO Unixware, Mac OS X.
13. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
14. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
15. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance.
16. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
17. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
18. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
19. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające muszą posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
20. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn.
21. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
22. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
23. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).

24. Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewnia stosowanie deduplikacji dla kopii zapasowych. Mechanizm zapewnia możliwość wykonywania spójnych kopii zapasowych serwerów aplikacyjnych (Microsoft SQL Server, Microsoft Exchange Server, Microsoft SharePoint Server) oraz replikację kopii zapasowych.
25. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
26. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
27. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
28. Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego Wykonawca dostarcza i wdraża na swój koszt. Wykonawca przeprowadzi instruktaże stanowiskowe i będzie świadczył asystę techniczną w zakresie umożliwiającym pracownikom jednostki Zamawiającego płynną obsługę wymienianego oprogramowania. Wdrożenie rozwiązania równoważnego nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy.

W ramach dostawy oprogramowania wirtualizacyjnego Wykonawca jest zobowiązany do przeprowadzenia usług zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w zakresie:

1. Aktywacja licencji oprogramowania wirtualizacyjnego na stronie producenta.
2. Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta.
3. Przygotowanie macierzy do podłączenia do systemu wirtualizacji – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta.
4. Instalacja oprogramowania wirtualizacyjnego na serwerach.
5. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów.
6. Konfiguracja i podłączenie serwerów wirtualizacyjnych do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii)  $n-(n-1)$  ścieżek, gdzie  $n$  oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy.
7. Konfiguracja i podłączenie serwerów wirtualizacyjnych do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii)  $n-(n-1)$  ścieżek, gdzie  $n$  oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN.
8. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q.
9. Przygotowanie koncepcji wirtualizacji fizycznych maszyn.

10. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym.
11. Konfiguracja klastra wysokiej dostępności:
  - a) Konfiguracja mechanizmów HA – w przypadku awarii węzła klastra wirtualne maszyny, które są na nim uruchomione muszą zostać przeniesione na sprawny węzeł klastra bez ingerencji użytkownika.
  - b) Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn.
  - c) Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera.
12. Weryfikacja działania klastra wysokiej dostępności.
13. Migracja istniejącej infrastruktury do środowiska wirtualnego.
14. Konfiguracja uprawnień w środowisku wirtualizacyjnym – integracja z usługą katalogową.
15. Konfiguracja powiadomień o krytycznych zdarzeniach (email).

### 4.3. Dostawa licencji na system backup (1 szt.).

Zamawiający posiada oprogramowania Veeam. Przedmiotem zamówienia jest przedłużenie i rozbudowa istniejącej u Zamawiającego licencji oprogramowania do backup Veem pozwalające na użytkowanie najnowszej wersji programu w okresie 24 miesięcy umożliwiających backup do 30 maszyn wirtualnych lub dostawy równoważnego systemu backup zgodnie z poniżej wskazanymi kryteriami równoważności.

Kryteria równoważności dla dostawy licencji przedłużającej i rozbudowującej oprogramowanie do backup Veem realizowanej przez dostawę równoważnego systemu wirtualizacji:

1. Wymagania ogólne:
  - a) licencja wieczysta na oprogramowanie ma umożliwiać backup środowiska wirtualnego z co najmniej dwóch serwerów 2-procesorowych obejmującego co najmniej 30 VM oraz 3 serwerach fizycznych;
  - b) oprogramowanie musi współpracować z infrastrukturą VMware oraz Microsoft Hyper-V;
  - c) oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami;
  - d) oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami;
  - e) oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V;
  - f) oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux;
2. Całkowite koszty posiadania:
  - a) oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej;
  - b) oprogramowanie musi tworzyć „samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków;
  - c) oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy;

- d) oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji;
- e) oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu;
- f) oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych;
- g) oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania,
- h) oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota;
- i) oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn i baz danych MS SQL;
- j) oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API;
- k) oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji;
- l) oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej;
- m) oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania;
- n) oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V;
- o) oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji konsol administracyjnych.

### 3. Wymagania RPO:

- a) oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
- b) oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
- c) oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji;
- d) oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty, które mogą zakłócić poprawne wykonanie backupu bez konieczności interakcji administratora;
- e) oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn

wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych;

- f) oprogramowanie musi posiadać wsparcie dla VMware vSAN;
- g) oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn;
- h) oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN;
- i) oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji;
- j) oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik;
- k) oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji.

#### 4. Wymagania RTO:

- a) oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
- b) dodatkowo dla środowiska vSphere powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna);
- c) oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny;
- d) oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere;
- e) oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków;
- f) oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny;
- g) oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej;
- h) oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites;
- i) oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
  - Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
  - Windows: NTFS, FAT, FAT32, ReFS;
- j) oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces;
- k) oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.

- l) oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
- m) oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects;
- n) oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2019 i nowszych
- o) oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska;
- p) oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego.

5. Ograniczenie ryzyka:

- a) oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
- b) oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
- c) oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
- d) oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec oraz ESET.

6. Monitoring:

- a) system musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich;
- b) system musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn;
- c) system musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej;
- d) system musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora;
- e) system musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej;
- f) system musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego;
- g) system musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

7. Raportowanie:

- a) system raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej;
- b) system musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V;



- c) system musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc;
  - d) system musi mieć możliwość ustawienia harmonogramu generowania raportów i eksportowania ich do formatów Microsoft Word, Microsoft Excel, Adobe PDF;
  - e) system musi mieć możliwość generowania raportów z dowolnego punktu w czasie i dostarczania go do określonych przez administratora odbiorców;
  - f) system w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów;
  - g) system musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury;
  - h) System musi mieć możliwość generowania raportu planowania pojemności;
  - i) system musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
8. Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego Wykonawca dostarcza i wdraża na swój koszt. Wykonawca przeprowadzi instruktaże stanowiskowe i będzie świadczył asystę techniczną w zakresie umożliwiającym pracownikom jednostki Zamawiającego płynną obsługę wymienianego oprogramowania. Wdrożenie rozwiązania równoważnego nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy.

W ramach dostawy oprogramowania backup Wykonawca jest zobowiązany do przeprowadzenia usług zaplanowania, uruchomienia oraz przetestowania środowiska backup, co najmniej w zakresie:

1. Instalacja i rekonfiguracja oprogramowania zarządzającego wykonywaniem kopii zapasowych na dostarczonym serwerze.
2. Aktywacja oraz instalacja niezbędnych licencji.
3. Konfiguracja stacji zarządzającej.
4. Dołączenie klientów do system backupu.
5. Zdefiniowanie zadań backupu oraz przypisanie do nich harmonogramu automatycznego wykonywania:
  - a) kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące;
  - b) kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy;
  - c) kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu;
  - d) kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową;
  - e) musi istnieć możliwość odtworzenia:
    - i. całej wirtualnej maszyny;
    - ii. dysku wirtualnej maszyny;
    - iii. pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa);
6. Zdefiniowanie powiadomień o przebiegu zadania (Zamawiający wymaga skonfigurowania powiadomień na wskazany adres email zawierających, co najmniej:

- a) Nazwę zadania backupu;
  - b) Status zakończenia zadania backupu /Powodzenie, niepowodzenie/;
  - c) Długość trwania zadania backupu;
  - d) Ilość zapisanych na taśmie danych;
7. Zdefiniowanie powiadomień na wskazany adres email o zdarzeniach:
- a) Błąd urządzenia;
  - b) Uszkodzenie wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi;
  - c) Brak miejsca w wewnętrznej bazie danych systemu zarządzania kopiami zapasowymi;
  - d) Konieczność przeprowadzenia oczyszczania wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi;
  - e) Zdarzenia dotyczące licencji;
  - f) Zapełnienia mail-słotu.
8. Uruchomienie testowych zadań backupu
9. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień email
10. Uruchomienie testowych zadań odtworzenia danych
11. Miejscem przechowywania kopii zapasowych jest:
- a) Serwer backupu;
  - b) NAS.
12. Wykonawca na etapie wdrożenia jest zobowiązany, aby ustalić czasy RPO (okresu przez jaki dane mogą być utracone w wyniku awarii) i RTO (okresu, w ciągu którego system, który uległ awarii powinien zostać przewrócony) z Zamawiającym.
13. System musi zostać podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na serwerze backupu.

#### 4.4. Dostawa licencji na program antywirusowy (150 szt.).

Zamawiający aktualnie posiada oprogramowanie antywirusowe ESET PROTECT Advanced. Przedmiotem zamówienia jest przedłużenie i rozbudowa istniejącej u Zamawiającego licencji oprogramowania antywirus ESET PROTECT Advanced pozwalające na użytkowanie najnowszej wersji programu w okresie 24 miesięcy umożliwiających korzystanie z oprogramowania na 150 urządzeniach końcowych z funkcją XDR lub dostawy równoważnego systemu antywirusowego zgodnie z poniżej wskazanymi kryteriami równoważności.

Kryteria równoważności dla dostawy licencji przedłużającej i rozbudowującej oprogramowanie antywirusowe realizowanej przez dostawę równoważnego systemu antywirusowego:

##### Administracja zdalna w chmurze.

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.

7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

#### Ochrona stacji roboczych.

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
  - a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
  - b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
  - c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
  - d. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
  - e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
  - a. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
  - b. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
  - c. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
  - d. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wydrebnionych z archiwum.

#### Ochrona serwera.

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.  
Dodatkowe wymagania dla ochrony serwerów Windows:
9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikację, czynność oraz adres IP.

17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.  
Dodatkowe wymagania dla ochrony serwerów Linux:
18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonoego mikro-serwisu.

#### Szyfrowanie.

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10/11 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych na komputerach z UEFI.

#### Ochrona urządzeń mobilnych opartych o system Android.

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
  - a. usunięcie zawartości urządzenia,
  - b. przywrócenie urządzenia do ustawień fabrycznych,
  - c. zablokowania urządzenia,
  - d. uruchomienie sygnału dźwiękowego,
  - e. lokalizację GPS.
  - f. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
  - g. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
    - h. nazwę aplikacji,
    - i. nazwę pakietu,
    - j. kategorię sklepu Google Play,
    - k. uprawnienia aplikacji,
    - l. pochodzenie aplikacji z nieznanego źródła.

### Ochrona serwera pocztowego MS Exchange.

1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.
2. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.
3. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
4. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
5. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
6. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
7. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
8. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
9. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
10. Rozwiązanie ma posiadać mechanizm greylisting (szara lista).
11. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

### Sandbox w chmurze.

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:

- a. Czysty,
  - b. Podejrzany,
  - c. Bardzo podejrzany,
  - d. Szkodliwy.
1. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wydrebnionych z archiwum.
  2. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
  3. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

#### Ochrona usługi Microsoft 365.

1. Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams.
2. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Microsoft 365.
3. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.
4. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.
5. Rozwiązanie musi być dostępny w języku polskim.
6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:
  - a. użytkowników, otrzymujących najwięcej spamu,
  - b. użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
  - c. użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
  - d. kont użytkowników, które mogą być podejrzane.
7. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.
8. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:
  - a. jaka ilość wiadomości została przeskanowana,
  - b. wynik skanowania poszczególnych wiadomości,
  - c. czynność podjęta przez rozwiązanie.
9. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o: zagrożeniach, które zostały wykryte,
  - a. na jakim koncie zostały wykryte,
  - b. jakie zagrożenie zostało wykryte,
  - c. podjętą czynność.
10. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.
11. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.
12. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
13. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:
  - a. wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
  - b. wprowadzenia białych i czarnych list adresów ochrony Exchange’a Online,



- c. dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
- 14. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
- 15. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
- 16. Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
- 17. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
- 18. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.

#### Moduł XDR.

- 1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
- 2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
- 3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
- 4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
- 5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
- 6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
- 7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
- 8. Serwer musi posiadać minimum 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
- 9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
- 10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
- 11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
- 12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
- 13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
- 14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
- 15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli

zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.

16. Konsola administracyjna musi mieć możliwość tagowania obiektów.

17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego Wykonawca dostarcza i wdraża na swój koszt. Wykonawca przeprowadzi instruktaże stanowiskowe i będzie świadczył asystę techniczną w zakresie umożliwiającym pracownikom jednostki Zamawiającego płynną obsługę wymienianego oprogramowania. Wdrożenie rozwiązania równoważnego nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy.

## 5. Przedmiot zamówienia dla części nr 2.

### 5.1. Dostawa licencji zapory sieciowej UTM (2 szt.).

W ramach działania przewiduje się zakup licencji usług subskrypcyjnych na dwa istniejące urządzenia UTM Fortigate FG-200F. Licencja musi umożliwić Zamawiającemu korzystanie z aktualnych baz funkcji ochronnych producenta i serwisów oraz obejmować kontrolę aplikacji, IPS, antywirus, antyspam, web filtering, funkcję DLP, funkcję ochrony przed zagrożeniami typu Zero-Day, umożliwienie zestawiania szyfrowanego połączenia poprzez bezpieczny tunel z urządzenia pracownika do sieci urzędu, serwerów i systemów dziedzinowych tam się znajdujących w okresie 24 miesięcy od dnia odbioru przedmiotu zamówienia. Licencja musi umożliwiać opcję dostarczenia sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia.

Zamawiający dopuszcza rozwiązanie równoważne w postaci dostawy dwóch innych urządzeń lub platformy bezpieczeństwa spełniających poniższe kryteria równoważności funkcjonalnej:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPsec VPN, Antywirus, IPS.

System musi wspierać IPv4 oraz IPv6 w zakresie:

1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.

Minimalne parametry techniczne jednego urządzenia:

1. Przepustowość Firewall: min. 27 Gbps.
2. Musi obsługiwać min. 3 000 000 jednoczesnych połączeń.
3. Musi obsługiwać co najmniej 2000 połączeń VPN.
4. Wydajność IPsec VPN min. 13 Gbps.
5. Wydajność SSL VPN: min. 2 Gbps.
6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3,5 Gbps.
8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4 Gbps.

9. Automatyczna aktualizacja plików sygnatur antywirusowych.
10. Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji.
11. Możliwość wsparcia IPS z poziomu urządzenia poprzez dodatkowe subskrypcje.
12. Automatyczna aktualizacja sygnatur IPS.
13. IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy.
14. Wsparcie dla wszystkich głównych protokołów: HTTP, FTP, SMTP, POP3.
15. Ilość interfejsów sieciowych: minimum 16 portów Gigabit Ethernet RJ-45 oraz minimum 2 porty 10-Gigabit Ethernet SFP+.
16. Wsparcie VLAN: Musi posiadać minimum 200 sieci VLAN.
17. Administracja urządzenia musi być możliwa poprzez graficzny interfejs zarządzania.
18. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
  - a. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
  - b. Kontrola Aplikacji.
  - c. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
  - d. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS oparta o mechanizmy sztucznej inteligencji.
  - e. Ochrona przed atakami - Intrusion Prevention System.
  - f. Kontrola stron WWW.
  - g. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
  - h. Zarządzanie pasmem (QoS, Traffic shaping).
  - i. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
  - j. Funkcja DLP chroniąca przed utratą danych poprzez ich identyfikację oraz blokowanie, gdy są przesyłane na zewnątrz sieci.
  - k. Funkcja ochrony przed zagrożeniami typu Zero-Day.
  - l. Analiza ruchu szyfrowanego protokołem SSL.
  - m. Analiza ruchu szyfrowanego protokołem SSH.
19. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
20. Zapewnienie obsługi Routingu statycznego, Policy Based Routingu, protokołów dynamicznego routing w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
21. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
22. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
23. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
24. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
25. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

26. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
27. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
28. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
29. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
30. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
31. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
32. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
33. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
34. Rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
35. Urządzenie powinno mieć możliwość generowania raportów.
36. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
37. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
38. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
39. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
40. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
41. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
42. Wykonawca zapewni usługi wsparcia technicznego w okresie do dnia 8.04.2026 r. świadczone przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:
  - a. Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
  - b. Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
  - c. Doradztwo w zakresie konfiguracji.
  - d. Zdalne wsparcie techniczne.
  - e. Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
  - f. Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
  - g. Przygotowanie urządzenia do zdalnej konfiguracji.

- h. Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
  - i. Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
  - j. Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
  - k. Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.
43. Wykonawca zapewni licencje subskrypcyjne gwarantujące udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia.
44. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować następujące elementy: Kontrola Aplikacji, IPS, Antywirus, Antyspam, Antymalware, Web Filtering, Funkcja DLP, Funkcja ochrony przed zagrożeniami typu Zero-Day w okresie 24 miesięcy od dnia odbioru przedmiotu zamówienia.
45. Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego Wykonawca dostarcza i wdraża na swój koszt. Wykonawca przeprowadzi instruktaże stanowiskowe i będzie świadczył asystę techniczną w zakresie umożliwiającym pracownikom jednostki Zamawiającego płynną obsługę wymienianego oprogramowania. Wdrożenie rozwiązania równoważnego nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy.

W ramach dostawy licencji Wykonawca jest zobowiązany także do przeprowadzenia usług rekonfiguracji urządzeń, co najmniej w zakresie:

1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.
2. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta.
3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (Kontrola Aplikacji, IPS, Antywirus, Antyspam, Antymalware, Web Filtering, Funkcja DLP, Funkcja ochrony przed zagrożeniami typu Zero-Day).
4. Przygotowanie projektu włączenia urządzenia do sieci LAN urzędu.
5. Konfiguracja dostarczonych systemów Firewall:
  - a. Konfiguracja podstawowych parametrów,
  - b. Konfiguracja translacji adresów NAT,
  - c. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, macierze, itp.,
  - d. Konfiguracja inspekcji określonych protokołów sieciowych,
  - e. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall,
  - f. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym,
  - g. Testowanie działania bramy.
6. Konfiguracja modułów należących do systemu wykrywania włamań IPS:
  - a. Konfiguracja podstawowych parametrów,
  - b. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań,

- c. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego,
  - d. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym,
  - e. Testowanie działania ochrony IPS.
7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL.
    - a. Przypisanie adresu IP do zarządzania,
    - b. Konfiguracja inspekcji protokołów HTTP, HTTPS; SMTP, FTP, POP3,
    - c. Definicja reguł filtrowania/blokowania,
    - d. Integracja z systemem domenowym w celu weryfikacji nawiązywania połączenia poprzez nazwę użytkownika z domeny.
  8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej.
  9. Konfiguracja uwierzytelniania w oparciu o dostarczony moduł uwierzytelnienia.
  10. Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla: dedykowanych, stworzonych na przelaniach sieci VLAN.
  11. W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (moduł uwierzytelnienia), nie zaś o adresy IP, czy MAC.
  12. W każdej instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaże Zamawiający) dla każdej z poniższych funkcjonalności:
    - a. kontrola dostępu - zaporą ogniową klasy Stateful Inspection,
    - b. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar,
    - c. ochrona przed atakami - Intrusion Prevention System [IPS/IDS],
    - d. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM,
    - e. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP),
    - f. kontrola pasma oraz ruchu [QoS, Traffic shaping],
    - g. Kontrola aplikacji oraz rozpoznawanie ruchu P2P,
    - h. Ochrona przed wyciekiem poufnej informacji (DLP),
    - i. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL),
    - j. Inspekcja ruchu SSL,
    - k. Ochrony przed atakami na stacje klienckie,
    - l. Kontrola pasma.
  13. Konfiguracja szyfrowanych tuneli VPN (IPSec) pomiędzy lokalizacjami zdalnymi.
  14. Konfiguracja logowania i raportowania.
  15. Podłączenie klastra urządzeń UTM do dostarczanego oprogramowania do zbierania i przechowywania logów z urządzeń UTM.

## 5.2. Dostawa licencji oprogramowania do zbierania i przechowywania logów z urządzeń UTM (1 szt.).

Przedmiotem zamówienia jest przedłużenie istniejącej u Zamawiającego licencji oprogramowania do zbierania i przechowywania logów z urządzeń UTM FortiAnalyzer-VM Subscription License pozwalające na użytkowanie najnowszej wersji programu w okresie 24 lub dostawy równoważnego systemu wirtualizacji zgodnie z poniżej wskazanymi kryteria równoważności.

Kryteria równoważności dla dostawy licencji przedłużającej oprogramowanie do zbierania i przechowywania logów z urządzeń UTM FortiAnalyzer-VM Subscription License realizowanej przez dostawę równoważnego systemu do zbierania i przechowywania logów z urządzeń UTM:

1. System musi umożliwiać analizę sieci bezpieczeństwa poprzez korelację zdarzeń we wszystkich dziennikach i wykrywanie anomalii w czasie rzeczywistym z usługą wskaźnika narażenia (IOC) i wykrywaniem zagrożeń.
2. System musi umożliwiać integrację i korelację z dziennikami zdarzeń istniejących urządzeń UTM w celu uzyskania lepszej widoczności i krytycznych informacji o sieci.
3. System musi zapewniać wysoką dostępność poprzez automatyczne tworzenie kopii zapasowych bazy danych oprogramowania (do 4 węzłów), które mogą być rozproszone geograficznie na potrzeby odzyskiwania po awarii.
4. System musi zapewniać automatyzacja zabezpieczeń poprzez automatyzację za pomocą interfejsu API REST, skryptów automatyzacji, aby przyspieszyć odpowiedź w zakresie bezpieczeństwa.
5. System musi obsługiwać domeny wielodostępne i administracyjne (ADOMs) oraz oddzielać dane klientów i zarządzać domenami.
6. System musi obsługiwać wdrażanie urządzeń, maszyn wirtualnych, hostowanych lub w chmurze. Musi pozwalać na używanie AWS, Azure lub Google do archiwizacji dzienników jako dodatkowej pamięci masowej.
7. System musi umożliwiać wykrywanie trwałych zagrożeń (APTS), luk i wskaźników w czasie rzeczywistym.
8. System musi umożliwiać zbadanie podejrzanego wzorca ruchu i wyszukiwanie za pomocą filtrów predefiniowanych lub niestandardowych obserwacji zdarzeń w celu generowania powiadomień i monitorowania w czasie rzeczywistym dla operacji min. NOC i SOC, SD-WAN, SSL VPN, Wireless, Shadow IT, IPS, sieciowego zwolnienia.
9. System musi umożliwiać zautomatyzowaną reakcję na incydenty.
10. System musi umożliwiać monitorowanie do min. 10000 urządzeń oraz min. 5GB danych na dzień.
11. System musi umożliwiać monitorowanie i podgląd zapewniający wgląd w kontekst i znaczenie aktywności sieciowej, ryzyka, luki, próby ataku, wskaźniki kompromisu i anomalii aktywności użytkownika.
12. System musi zapewniać widok dziennika umożliwiający wykorzystanie filtrów wyszukiwania w zarządzanych dziennikach urządzeń, tworzenie dzienników z niestandardowymi widokami i grupami dzienników, w tym bazą danych SIEM.
13. System musi umożliwiać tworzenie raportów zawierających kompleksową analizę postawy bezpieczeństwa, w tym raporty dotyczące technologii operacyjnej (OT), ocenę bezpieczeństwa, ocenę bezpieczeństwa dla PCI, Secure SD-WAN, VPN, wykrywanie anomalii sieci.
14. Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego Wykonawca dostarcza i wdraża na swój koszt. Wykonawca przeprowadzi instruktaże stanowiskowe i będzie świadczył



asystę techniczną w zakresie umożliwiającym pracownikom jednostki Zamawiającego płynną obsługę wymienianego oprogramowania. Wdrożenie rozwiązania równoważnego nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy.

## 6. Przedmiot zamówienia dla części nr 3.

### 6.1. Dostawa licencji oprogramowania do monitorowania i analizy cyberbezpieczeństwa (1 szt.).

Przedmiotem zamówienia jest dostawa licencji i wdrożenie systemu przeciwdziałania cyberzagrożeniom oferujący możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację obsługi.

Minimalne parametry funkcjonalne oprogramowania:

1. System musi umożliwić odbieranie logów z urządzeń sieciowych oraz wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje minimum następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.
2. System musi zapewnić agentów na stacje końcowe umożliwiających im pobieranie pełnych danych hostów, których chronią i przesłanie tych danych do systemu centralnego w celu dalszej korelacji i analizy behawioralnej. W przypadku wykrycia zagrożenia agenci muszą umożliwiać automatyczną i dostosowaną do kontekstu reakcję, m.in. blokowanie bądź izolację sieciową złośliwego oprogramowania.
  - 2.1. Agent musi posiadać możliwość dodawania i usuwania reguł wbudowanego firewalla obejmując m.in. blokowanie i odblokowywanie poszczególnych procesów bądź reguł dotyczących ruchu sieciowego stanowiące reakcję na wykryte zagrożenie.
  - 2.2. Agent musi pobierać oraz aktualizować na bieżąco listę zainstalowanego oprogramowania.
  - 2.3. System w przypadku wykrycia techniki ataku ukierunkowanego na podatną aplikację w celu zablokowania ataku musi umożliwiać zatrzymanie procesu aplikacji oraz zapewnić dostęp do danych dowodowych obejmujących nazwę chronionego systemu, system operacyjny, tożsamość użytkownika, nazwę procesu, dokładną komendę uruchamiającą złośliwy proces wraz parametrami i znacznik czasowy.
  - 2.4. System musi obsługiwać scenariusz uwzględniający ocenę prawdopodobieństwa materializacji się wykrytego zagrożenia, gdzie w przypadku, gdy wyliczone przez system prawdopodobieństwo ataku jest wysokie proces zostanie zablokowany, natomiast w pozostałych przypadkach, gdy jest ono średnie bądź niskie zostanie on zamrożony z możliwością ponownego wznowienia przez operatora.
  - 2.5. System musi posiadać możliwość dostosowania reakcji na zagrożenie w zależności od rodzaju zasobu, który chroni, przykładowo, jeżeli zagrożenie dotyczyć będzie procesu na stacji roboczej proces zostanie automatycznie zablokowany, jednakże w przypadku, gdy to samo zagrożenie dotyczyć będzie serwera świadczącego usługi w sieci publicznej proces pozostanie uruchomiony z jednoczesną blokadą publicznego ruchu przychodzącego.
3. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz

obsługi zapytań WQL w ramach protokołu WMI.

4. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.
5. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiające ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie.
6. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorce wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.
7. Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych.
8. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware.
9. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.
10. System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku, gdy będzie to konieczne przywrócić jedną z poprzednich wersji.
11. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg” znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX.
12. Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni, w której te logi są przesyłane. Przykładowo, jeżeli logi są przesyłane w standardzie CEF system dobierze odpowiedni parser, w przypadku, gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora.
13. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej.
14. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zawartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo, jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku, gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B.
15. Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie.
16. System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in.

- odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów.
17. Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielania ich składowania na osobny serwer i dedykowane zasoby dyskowe.
  18. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.
  19. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych.
  20. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach.
  21. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości.
  22. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa.
  23. Elektroniczna dokumentacja musi posiadać możliwość wizualizacji, gdzie widoczne będą urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. Wybór na dowolny z obiektów musi pozwolić na podgląd oraz edycję parametrów tego obiektu.
  24. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej.
  25. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci.
  26. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły.
  27. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.
  28. Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o minimum następujące informacje:
    - a. nowe zasoby wykryte w sieci,
    - b. typy wykrytych zasobów (np.: serwer lub stacja robocza),
    - c. zastosowane na nich zabezpieczenia,
    - d. usługi, z którymi się komunikują,

- e. nowe usługi wykryte na zasobie
  - f. komunikację do usług wykrytych na zasobie.
29. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację.
  30. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora.
  31. Interfejs graficzny musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi, której ta komunikacja dotyczy.
  32. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać minimum następujące typy wskaźników:
    - a. fqdn,
    - b. e-mail,
    - c. nazwa pliku,
    - d. ścieżka do pliku,
    - e. hash,
    - f. adres IP,
    - g. klucz rejestru,
    - h. cmd.
  33. System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest, aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (<https://www.misp-project.org/>).
  34. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu.
  35. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”).
  36. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych.
  37. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.
  38. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności.
  39. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.
  40. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie.

41. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w zakresie minimum:
  - a. id techniki,
  - b. taktykę,
  - c. platformy których dotyczy,
  - d. potencjalne źródła,
  - e. opis zagrożenia,
  - f. mityzację,
  - g. sposób detekcji,
  - h. referencje.
42. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.
43. Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielanie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy).
44. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum:
  - a. rozdzielanie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych,
  - b. rozdzielanie procesu nauczania zachowania stacji roboczych od serwerów,
  - c. rozdzielanie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji,
  - d. rozdzielanie procesu nauczania serwerów należących do domeny od pozostałych serwerów.
45. System uczenia maszynowego musi posiadać wbudowane mechanizmy niewymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA).
46. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji.
47. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.
48. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację.
49. System musi posiadać interfejs graficzny do tworzenia własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenia reguł musi uwzględniać minimum:

- a. sparsowane pola oraz ich wartości,
  - b. listy referencyjne,
  - c. atrybuty użytkowników z Active Directory,
  - d. atrybuty komputerów z Active Directory,
  - e. bazę wskaźników kompromitacji (IOC),
  - f. informacje z elektronicznej dokumentacji,
  - g. anomalie w zachowaniu użytkowników (UBA),
  - h. anomalie w zachowaniu zasobów (EBA),
  - i. podatności na zasobach,
  - j. wyniki analizy konfiguracji,
  - k. techniki MITRE ATT&CK®.
50. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić minimum:
- a. wykrycie dowolnej treści w logach,
  - b. wykrycie zmiany jednego z kilku pól,
  - c. wykrycie zaniku wiadomości,
  - d. wykrycie nowej wartości pola w zadanym okresie,
  - e. wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności,
  - f. wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie,
  - g. wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie,
  - h. wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa,
  - i. wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie,
  - j. wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie,
  - k. wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa,
  - l. wykrycie ilości uruchomionych procesów w zadanym okresie,
  - m. wykrycie skanowania portów.
51. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić minimum:
- a. wykrycie wystąpienia wartości pola na wybranej liście,
  - b. wykrycie niewystępowania wartości pola na wybranej liście,
  - c. wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku, z którego został uruchomiony),
  - d. wykrycie niewystąpienia pary wartości na wybranej liście (np.: nazwa użytkownika wraz aplikacją z którą się wcześniej nie łączył).
52. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić minimum:
- a. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory,
  - b. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory,
  - c. wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta).
  - d. wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins),

- e. wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej.
53. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić minimum:
- a. wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory,
  - b. wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory,
  - c. wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej.
54. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić minimum:
- a. wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji;
  - b. wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji;
  - c. wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji.
55. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić:
- a. wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu,
  - b. wykrycie połączenia do usługi przez nieautoryzowanego użytkownika,
  - c. wykrycie nieautoryzowanej usługi na serwerze,
  - d. wykrycie nieautoryzowanego połączenia do usługi na serwerze,
  - e. wykrycie nieautoryzowanego połączenia z serwera usług,
  - f. wykrycie nieautoryzowanego połączenia do sieci Internet.
56. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić minimum:
- a. wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak DDoS lub próbę propagacji złośliwego oprogramowania,
  - b. wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware,
  - c. wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejęcie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie,
  - d. wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.
57. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić minimum:
- a. wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak DDoS lub próbę propagacji złośliwego oprogramowania,
  - b. wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware,
  - c. wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejęcie komputera przez cyberprzestępcę lub złośliwe oprogramowanie,
  - d. wykrycie anomalii związanych z procesami uruchamianymi na serwerach.
58. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić minimum:
- a. wykrycie skanowania portów z zasobu posiadającego krytyczne podatności,
  - b. wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności,
59. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać minimum na:

- a. wykrycie wielokrotnych prób nieudanego logowania do komputera,
  - b. wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł niespełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.
60. Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić minimum:
- a. wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
  - b. wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
  - c. wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie.
61. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając minimum:
- a. wykrycie anomalii na koncie uprzywilejowanym użytkownika,
  - b. wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej,
  - c. wykrycie wielu typów anomalii na komputerze z krytyczną podatnością,
  - d. wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi,
  - e. wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.
62. System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki. Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora.
63. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać:
- a. sparsowane pola oraz ich wartości,
  - b. atrybuty użytkowników z Active Directory,
  - c. atrybuty komputerów z Active Directory,
  - d. informacje z elektronicznej dokumentacji.
64. Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się minimum po:
- a. adresie IP,
  - b. koncie domenowym użytkownika,
  - c. strefie bezpieczeństwa,
  - d. zakresie adresów IP.
65. Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego.
66. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń.



67. Zdarzenia muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących minimum:
- wszystkie skorelowane zdarzenia,
  - korespondencja pocztowa,
  - załączniki z próbkami lub dowodami,
  - wskaźniki kompromitacji (IoC),
  - informacje pozyskane z innych systemów.
68. System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielania uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora.
69. Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane minimum następujące dane:
- identyfikacja celu i źródła zagrożenia,
  - nazwa oraz adres IP źródła zagrożenia,
  - rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza,
  - lokalizacja, z której pochodzi zagrożenie np.: Internet,
  - strefa bezpieczeństwa z której pochodzi zagrożenie,
  - prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło,
  - wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification),
  - nazwa oraz adres IP celu zagrożenia,
  - zabezpieczenia lokalne chroniące cel zagrożenia,
  - strefa bezpieczeństwa w której znajduje się cel zagrożenia.
70. Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń.
71. Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami.
72. Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w zakresie minimum:
- nazwy zasobu,
  - rodzaju zasobu,
  - ważności zasobu dla organizacji,
  - rodzaj przetwarzanych informacji,
  - usług, które ten zasób świadczy,
  - lokalizację użytkowników, którzy z niego korzystają,
  - usługi, z których zasób korzysta.
73. System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS).

Kwalifikacja musi uwzględniać minimum: dostępność operatora, jego obciążenia oraz parametry zasobu, którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług.

74. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń w zakresie minimum:
- nowe zdarzenie – jako zdarzenie zarejestrowane w systemie,
  - segregacja – segregacja i kwalifikacja zdarzeń,
  - incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa,
  - fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm,
  - zdarzenie obsłużone – zdarzenie, które zostało obsłużone w systemie.
75. System musi także zapewniać możliwość edycji w zakresie dodawania lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa” do statusu „zdarzenie zamknięte”, ale zablokować zmianę ze statusu „incydent bezpieczeństwa” na status „fałszywy alarm”.
76. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi.
77. System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia, z którym są grupowane oraz synchronizować z nim statusy. Dla zdarzeń przetwarzanych przez operatora, zmiana statusu głównego zdarzenia musi wymusić zmianę statusu pozostałych.
78. Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów.
79. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów.
80. W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi.
81. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell) na skonfigurowanie nowych integracji z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API.
82. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na:
- podgląd aktywności zagrożonego zasobu na linii czasu,
  - w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku,
  - w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu,
  - podgląd reguły korelacyjnej, która wygenerowała zdarzenie,
  - w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis,
  - listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich,
  - gotowe i proste w użyciu filtry rozszerzające analizę zdarzeń o:
    - listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po,

- listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym,
- h. gotowe i proste w użyciu filtry rozszerzające analizę logów o:
- listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym,
  - listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.
83. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:
- a. warunki powiadomień, w tym:
    - zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
    - zdarzeń o przekroczonych czasach SLA o definiowalny okres,
    - zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
    - zdarzeń, których priorytet osiągnął określoną wartość,
    - zdarzeń zakwalifikowanych jako incydent bezpieczeństwa,
    - zdarzeń, na których doszło do naruszenia bezpieczeństwa,
    - zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną,
    - zdarzeń realizujących zdefiniowaną usługę,
    - zdarzeń przetwarzających sklasyfikowane informacje,
    - zdarzeń przetwarzanych na krytycznych zasobach,
  - b. odbiorców powiadomień, w tym:
    - operatora, któremu zostało przydzielone zdarzenie,
    - właściciela zasobu, na którym wystąpiło zdarzenie,
    - zespół obsługi, który odpowiada za obsługę zdarzeń,
    - właściciela usługi, która jest realizowana na zasobie, na którym wystąpiło zdarzenie,
    - podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną.
  - c. kanały powiadomień, m.in. e-mail, sms, komunikator,
  - d. zastosowanie mechanizmów grupowania:
    - grupowanie wielu powiadomień w jednej wiadomości,
    - ograniczenie liczby wierszy powiadomienia do określonej wartości.
84. System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku, gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:
- a. utworzenia nowego zdarzenia z określonym priorytetem,
  - b. utworzenia nowego zdarzenia na zasobie krytycznym,
  - c. utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę,
  - d. utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe,
  - e. utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej,
  - f. modyfikacji przydzielonego operatorowi zdarzenia przez innego operatora,
  - g. zamknięcia przydzielonego operatorowi zdarzenia przez innego operatora,
  - h. przejęcia przydzielonego operatorowi zdarzenia przez innego operatora.
85. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego:
- a. wybór raportu, który ma zostać wysłany,
  - b. zdefiniowanie jego tytułu,
  - c. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,

- d. możliwość ograniczenia cyklu do dni powszednich,
  - e. określenie daty przesłania pierwszego raportu,
  - f. możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do:
    - zdefiniowanej daty końcowej,
    - określonej liczby raportów,
  - g. określenie odbiorców raportu.
86. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi.
87. Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczają dla podatności wymagających obsługi priorytet w oparciu o następujące parametry:
- a. strefę bezpieczeństwa w której została wykryta podatność,
  - b. prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie,
  - c. rodzaj zasobu, którego dotyczy ta podatność,
  - d. ważność tego zasobu dla organizacji,
  - e. przetwarzane na tym zasobie informacje,
  - f. usługi realizowane przez ten zasób,
  - g. wartość parametrów CVSS dla podatności,
  - h. poprawność konfiguracji zasobu, na którym została wykryta podatność,
  - i. szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu.
88. W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi jak i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.
89. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach:
- a. wyliczonym priorytecie podatności,
  - b. aktualnym statusie obsługi,
  - c. ważności zasobu, na którym została wykryta,
  - d. adresie IP tego systemu,
  - e. parametrów SLA związanych z tym statusem,
  - f. przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe,
  - g. parametrach CVSS, np.: lista podatności których „Access Complexity (AC)” = „low” oraz „Access Vector (AV)” = „Network”.
90. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach:
- a. przekroczenia czasu reakcji o określony czas np.: o godzinę,
  - b. możliwości przekroczenia czasu reakcji, np.: została godzina, aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji,
  - c. przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe,
  - d. przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym,

- e. przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę,
  - f. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe,
  - g. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych,
  - h. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę,
  - i. przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe,
  - j. przekroczenia czasu reakcji dla podatności na zasobie krytycznym,
  - k. przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę,
91. Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:
- a. warunki powiadomień,
    - podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
    - podatności o przekroczonych czasach SLA o definiowalny okres,
    - podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
    - podatności, których priorytet osiągnął określoną wartość,
    - zdarzeń realizujących zdefiniowaną usługę,
    - zdarzeń przetwarzających sklasyfikowane informacje,
    - zdarzeń przetwarzanych na krytycznych zasobach,
  - b. odbiorców powiadomień, w tym:
    - operatora, któremu została przydzielona podatność,
    - właściciela zasobu, na którym wystąpiła podatność,
    - zespół obsługi, który odpowiada za obsługę podatności,
    - właściciela usługi, która jest realizowana na zasobie, na którym wystąpiła podatność,
    - podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną.
  - c. kanały powiadomień, m.in. e-mail, sms, komunikator,
  - d. zastosowanie mechanizmów grupowania:
    - grupowanie wielu powiadomień w jednej wiadomości,
    - ograniczenie liczby wierszy powiadomienia do określonej wartości.
92. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku, gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:
- a. przydzielenia nowej podatności do obsługi z określonym priorytetem,
  - b. przydzielenia nowej podatności do obsługi na zasobie krytycznym,
  - c. przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę,
  - d. przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe,
  - e. modyfikacji przydzielonej operatorowi podatności przez innego operatora,
  - f. zamknięcia przydzielonej operatorowi podatności przez innego operatora,
  - g. przejścia przydzielonej operatorowi podatności przez innego operatora.
93. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na:

- a. wybór raportu, który ma zostać wysłany,
  - b. zdefiniowanie jego tytułu,
  - c. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
  - d. możliwość ograniczenia cyklu do dni powszednich,
  - e. określenie daty przestania pierwszego raportu,
  - f. określenie okresu przez jaki będą one przesyłane, poprzez:
    - zdefiniowanie daty końcowej,
    - bez daty końcowej,
    - określenie liczby raportów,
  - g. określenie odbiorców raportu.
94. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji umożliwiające dostosowanie zakresu i prezentacji danych do potrzeb zalogowanego użytkownika.
95. System musi pozwalać na tworzenie dedykowanych:
- a. zestawów wykresów dla bieżącego użytkownika,
  - b. zestawów wykresów dla wybranego użytkownika,
  - c. zestawów wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu,
  - d. zestawów wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).
96. System musi zapewniać predefiniowane zestawy wykresów obejmujących następujące wykresy:
- a. wykres przedstawiający status klasyfikacji zdarzeń,
  - b. wykres przedstawiający skalę zagrożeń,
  - c. wykres przedstawiający źródła zagrożeń,
  - d. wykres przedstawiający poziom zagrożeń,
  - e. wykres przedstawiający czas obsługi zagrożeń,
  - f. wykres przedstawiający zagrożone usługi,
  - g. wykres przedstawiający skalę podatności,
  - h. wykres przedstawiający czas obsługi podatności,
  - i. wykres przedstawiający wagę podatności, który uwzględnia:
97. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.
98. Interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem.
99. Oferowana licencja nie może nakładać limitów w zakresie ilości danych przekazywanych do systemu, tj. EPS (Events Per Second).
100. System musi umożliwiać równoczesną pracę co najmniej 5 operatorów oraz obsługiwać co najmniej 200 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych funkcjonalności.
101. Dla wszystkich źródeł objętych licencją oraz stanowiących jednocześnie komputery bądź serwery licencja produktu musi uwzględniać możliwość wykorzystania dedykowanych agentów XDR.
102. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.
103. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie

funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet.

104. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows Server (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).

Wdrożenie oprogramowania do monitorowania i analizy cyberbezpieczeństwa – wymagania minimalne:

1. Wykonawca przeprowadzi instalację i konfigurację systemów operacyjnych dla serwerów wirtualnych na potrzeby zaoferowanego systemu.
2. Instalacja oprogramowania systemu serwerowego wraz z niezbędnymi usługami oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Zamawiającego).
3. Proces wdrożenia systemu określony powinien zostać zrealizowany zgodnie z opisanymi niżej wytycznymi oraz zatwierdzonym harmonogramem, umożliwiając efektywne wdrożenie rozwiązania w okresie 90 dni.
4. Proces wdrożeniowy powinien uwzględnić następujące obszary:
  - a. Obszar Analizy, zakładający stworzenie elektronicznej dokumentacji organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji (budowa kontekstu organizacji).
  - b. Obszar Detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowania modułu SIEM.
  - c. Obszar Reakcji, zakładający podłączenie i konfigurację mechanizmów wspomagających proces automatyzacji reakcji na wykryte zdarzenia, incydenty bezpieczeństwa i podatności w ramach zainstalowania modułu SOAR.

Obszar Analizy ma na celu identyfikację potencjalnych cyberzagrożeń oraz możliwych konsekwencji na jakie narażona jest organizacja. Zakres prac powinien uwzględniać minimum:

1. Pracę z konsultantem (w zakresie m.in. wprowadzenia do metodyki, uzupełnienia ankiety przedwdrożeniowej oraz przygotowania i zatwierdzenia harmonogramu prac).
2. Uruchomienie systemu w infrastrukturze zamawiającego, w tym:
  - a. konsultacje w przygotowaniu infrastruktury Zamawiającego do instalacji systemu,
  - b. przygotowanie przez Zamawiającego połączenia zdalnego,
  - c. instalację lub import maszyny wirtualnej typu „software appliance”,
  - d. aktywację licencji,
  - e. wstępną konfigurację,
  - f. import/wprowadzenie tabeli adresacji znaczących stref bezpieczeństwa, wymaganych przez mechanizmy wykrywania (np.: sieci serwerów, sieci DMZ, sieci LAN).
3. Podłączenie głównego źródła zdarzeń opisującego komunikację sieciową, w tym:
  - a. przekierowanie logów opisujących transmisje sieciową (traffic) z zapór sieciowych (Firewall) na kolektor systemu,
  - b. uruchomienie reguł wykrywania.
4. Prace audytowe, w tym:
  - a. pasywną analizę transmisji sieciowej:

- i. o ruch z/do serwerów webowych i aplikacyjnych,
    - ii. o ruch z/do serwerów baz danych,
    - iii. o ruch z/do serwerów pocztowych,
    - iv. o ruch z/do kontrolerów domenowych,
    - v. o ruch z/do serwerów usług podstawowych (m.in. DNS/NTP),
    - vi. o ruch z/do zasobów zidentyfikowanych na bazie charakterystyki i wolumenu ruchu oraz możliwości identyfikacji aplikacji.
  - b. konsultacje w ramach otrzymanych wyników,
  - c. zebranie danych audytowych wymaganych do sporządzenia raportu.
5. Analizę podatności, w zakresie:
- a. integracji po API ze wskazanym przez zamawiającego komercyjnym skanerem/ skanerami podatności lub zainstalowanie skanera podatności typu open source,
  - b. przygotowanie reguł priorytetów i importu krytycznych podatności.
6. Przygotowanie dynamicznego raportu audytowego w oparciu o dostępne w systemie narzędzia elektronicznej dokumentacji i szacowania ryzyka obejmującego analizę prawdopodobieństwa przełamania zabezpieczeń organizacji. Raport powinien zawierać:
- a. zidentyfikowane zagrożenia oraz prawdopodobieństwo ich wystąpienia,
  - b. potencjalne wektory ataków dla wykrytych zagrożeń,
  - c. wizualizacja graficzna wykrytych źródeł zagrożeń oraz wektorów ataków,
  - d. rekomendacja zabezpieczeń,
  - e. zidentyfikowane zagrożenia związane z podatnościami oraz prawdopodobieństwo wykorzystania ich do przełamania zabezpieczeń.

Obszar Detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń. Zakres prac powinien uwzględniać minimum:

1. Podłączenie (przekierowanie przez Zamawiającego do systemu) źródeł zdarzeń i ich dalszą konfigurację w systemie. Kluczowe źródła zdarzeń obejmują:
  - a. zapory sieciowe w punktach styku z siecią Internet (Firewall brzegowy),
  - b. sieciowe systemy bezpieczeństwa dedykowane do wykrywania incydentów bezpieczeństwa (np.: Sandbox, IDP/IPS, AntySpam),
  - c. centralne systemy, dedykowane do kontroli złośliwego oprogramowania na stacjach końcowych/Serwerach, umożliwiające wykrywanie aktywności złośliwego oprogramowania (np.: AntyWirus, EDR),
  - d. kontroler domenowy oraz system zarządzania dostępem uprzywilejowanym,
  - e. systemy detekcji anomalii w przepływach lub zdarzeniach (np.: NBA),
  - f. system SIEM,
  - g. źródła, muszą zostać powiązane z parserami, pozwalającymi na detekcję zgodną z wbudowanymi w system regułami korelacji,
2. Adaptację reguł profilowych, pozwalających na dostosowanie zdarzeń do zasobów, których dotyczą.
3. Podłączenie reguł detekcji.
4. Podłączenie i konfiguracja mechanizmów UEBA:
  - a. integracja z Active Directory,
  - b. adaptacja profili użytkowników UBA,
  - c. adaptacja profili hostów EBA,



- d. import reguł bezpieczeństwa UEBA, uruchomienie procesu uczenia.

Obszar Reakcji ma na celu uruchomienie i dostrojenie mechanizmów automatyzacji w działaniach reagowania na wykryte zagrożenia bezpieczeństwa. Zakres prac powinien uwzględniać minimum:

1. Import gotowych scenariuszy obsługi.
2. Konfigurację zespołów obsługi, celem właściwej adresacji podatności oraz zdarzeń wymagających obsługi.
3. Konfigurację mechanizmów powiadamiania.
4. Usługa konsultacji powdrożeniowej, świadczona przez dedykowanego inżyniera w ramach okresu wsparcia musi w szczególności uwzględniać:
  - a. przygotowanie i modyfikację formularzy raportów;
  - b. tworzenie i edycję parserów;
  - c. przygotowywanie nowych reguł bezpieczeństwa;
  - d. modyfikację dostępnych reguł i ich dostrojenie;
  - e. wsparcie w procesie aktualizacji systemu;
  - f. tworzenie i edycję nowych scenariuszy reakcji.
5. Wykonawca musi zapewnić usługę obejmującą proces aktualizacji oprogramowania oraz kontekstu systemu (dotyczy to zwłaszcza bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji). Dostęp do centralnej usługi aktualizacyjnej ma pozwalać na automatycznie wyświetlanie i pobieranie z poziomu interfejsu systemu dostępnych aktualizacji. Dla pobranych w procesie aktualizacji reguł oraz parserów musi być dostępne wersjonowanie, pozwalające uruchomić nową wersję reguły korelacyjnej oraz parsera z poziomu interfejsu systemu. Automatyczne wersjonowanie ma umożliwiać wczytanie starszej wersji reguły lub parsera, a zmiana reguł i parserów musi być możliwa z poziomu graficznego systemu.

## 6.2. Zakup usług szkoleń z zakresu oprogramowania do monitorowania i analizy cyberbezpieczeństwa (30 godz.).

Wykonawca zapewni szkolenia w wymiarze 30 efektywnych godzin zegarowych w zakresie użytkowania i administrowania wdrożonego systemu dotyczący minimum: instalacji, konfiguracji w zakresie zbierania i przechowywania logów, tworzenia reguł korelacyjnych w celu wykrywania cyberzagrożeń, tworzenia automatycznych reguł do szczegółowej analizy potencjalnych incydentów bezpieczeństwa, konfiguracja powiadomień o wykrytych incydentach, parametryzację systemu. Szkolenie musi być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydany przez producenta systemu.

1. Szkolenia będą trwały maksymalnie 6 godzin szkoleniowych w ciągu dnia.
2. Szkolenia będą odbywać się w dni robocze w godzinach 8.30 – 14.30.
3. Szkolenia będą prowadzone w języku polskim w formule stacjonarnej w siedzibie Zamawiającego. Zamawiający dopuszcza prowadzenie szkoleń w trybie zdalnym w formule on-line.
4. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 14 dni przed rozpoczęciem szkolenia.

5. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę.
6. W przypadku szkoleń trwających do 3 godzin, przewiduje się jedną przerwę trwającą 15 minut. W przypadku szkoleń trwających powyżej 3 godzin, organizowane będą dwie przerwy trwające 15 minut każda. Dodatkowo, w przypadku szkoleń trwających 6 godzin zaplanowana jest przerwa trwająca 30 minut. Przerw nie wlicza się do czasu efektywnego szkolenia.
7. W ramach organizacji szkoleń Zamawiający zapewni rekrutację osób biorących udział w szkoleniach. Wykonawca jest zobowiązany do przeprowadzenia szkolenia uzupełniającego dla osób, które nie ze względów przypadków losowych nie będą mogły uczestniczyć w szkoleniu w wyznaczonych terminach.
8. W ramach organizacji szkoleń Wykonawca zapewni:
  - a. Materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty informacyjne, broszury) w formie papierowej lub elektronicznej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Ponadto w przypadku organizacji szkoleń w formule stacjonarnej (w siedzibie Zamawiającego), uczestnicy otrzymają materiały pisarskie, w tym zeszyty, długopisy, ołówki itp. Materiały szkoleniowe przekazywane są nieodpłatnie uczestnikom na własność. 2 egzemplarze materiałów szkoleniowych zostaną przekazane Zamawiającemu w celach archiwalnych.
  - b. W przypadku szkoleń prowadzonych w trybie zdalnym w formule on-line Wykonawca jest zobowiązany dostarczyć narzędzia do komunikacji zdalnej, które umożliwią dwustronne przesyłanie przez sieć Internet obrazu i dźwięku między prowadzącym szkolenie a uczestnikami szkolenia. Narzędzie musi umożliwiać zadawanie pytań także w formie pisemnej bezpośrednio na czacie w trakcie trwania sesji szkoleniowej. W przypadku szkolenia prowadzonego w trybie zdalnym w formule on-line Zamawiający zastrzega możliwość nagrania szkolenia, a Wykonawca musi zapewnić wyrażenie na to zgody osoby prowadzącej szkolenie.
  - c. W przypadku szkoleń stacjonarnych (w siedzibie Zamawiającego) oraz o ile wynika to z programu szkolenia Wykonawca zapewni sprzęt komputerowy dla każdego uczestnika szkolenia umożliwiający przeprowadzenie szkolenia oraz wystarczającą liczbę własnych licencji na oprogramowanie komputerowe wykorzystywane przy realizacji szkoleń.
  - d. Projektor multimedialny, tablice i inne artykuły niezbędne do prowadzenia szkoleń w przypadku prowadzenia szkoleń stacjonarnych (w siedzibie Zamawiającego).
  - e. Właściwe działania promocyjne i informacyjne dotyczące szkoleń, w tym właściwe oznakowanie sal szkoleniowych, jak również oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych uczestnikom oraz Zamawiającemu w celach archiwalnych obowiązkowymi oznaczeniami Beneficjentów Funduszy Europejskich.
  - f. Wydanie uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.
  - g. Kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.
  - h. Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:
    - Lista obecności uczestników szkolenia (dziennie, wypełniane oddzielnie każdego dnia szkolenia).
    - Lista odbioru zaświadczeń o ukończeniu szkolenia.

- Potwierdzenie przez uczestników odbioru materiałów szkoleniowych.
- Przeprowadzenie ankiet satysfakcji po każdym szkoleniu.